

**IN THE CLAIMS:**

- 1 1. (Currently Amended) Method for comparing a first content with a second content to  
2 determine whether the contents are identical, comprising:  
3       storing the first content in a cache on a local storage system;  
4       requesting a second content from a remote storage system, wherein the second  
5 content is stored in a network storage arrangement on the remote storage system;  
6       identifying a protocol encoding the first content and second content;  
7       computing a first signature of the first content and a second signature of the sec-  
8 ond content, wherein the first signature has one or more unique protocol markers that are  
9 generated from transformation during protocol encoding and the second signature has one  
10 or more unique protocol markers that are generated from transformation during protocol  
11 encoding;  
12       comparing the one or more unique protocol markers of the first computed signa-  
13 ture with the one or more unique protocol markers the second signature to determine  
14 whether the first content is identical to the second content; and  
15       storing ~~in~~ the second content in the cache on the local storage system, in response  
16 to determining the first content is not identical to the second content.
- 1 2. (Previously Presented) The method of claim 1 further comprising:  
2       selecting a first set of data segments from the first content and a second set of data  
3 segments from the second content; and  
4       using the selected first set of data segments and the second set of data segments to  
5 compute the first signature and the second signature.
- 1 3. (Original) The method of claim 2 wherein the selected first set of data segments and  
2 second set of data segments comprise locations associated with one or more protocol  
3 markers.

- 1 4. (Previously Presented) The method of claim 1 wherein the step of computing the sig-  
2 nature of the first content and the signature of the second content further comprises:  
3 identifying the one or more protocol markers associated with the first content; and  
4 identifying the one or more protocol markers associated with the second content.
- 1 5. (Original) The method of claim 4 wherein the one or more protocol markers associ-  
2 ated with the first content comprises discrete cosine coefficients.
- 1 6. (Original) The method of claim 4 wherein the one or more protocol markers associ-  
2 ated with the second content comprises discrete cosine coefficients.
- 1 7. (Original) The method of claim 4 wherein the one or more protocol markers associ-  
2 ated with the first content comprises motion vectors.
- 1 8. (Original) The method of claim 4 wherein the one or more protocol markers associ-  
2 ated with the second content comprises motion vectors.
- 1 9. (Previously Presented) The method of claim 4 further comprising:  
2 identifying a length of the first content; and  
3 identifying a length of the second content.
- 1 10. (Currently Amended) A system to compare a first content with a second content, t  
2 comprising:  
3 a content comparator executing on a local storage-system-server, the content com-  
4 parator contains:  
5 a protocol identification module configured to identify a first protocol as-  
6 sociated with the first content and a second protocol associated with the second  
7 content, wherein the second content is stored on a remote storage-system-server,

8 | where the remote storage-system-server stores the second content and other data in  
9 | a network area storage arrangement,

10 | a plurality of data segmentation modules configured to select a set of data  
11 | segments from each of the first content and the second content,

12 | a plurality of signature computation modules configured to generate a first  
13 | signature of the first content and a second signature of the second content,  
14 | wherein the first signature has one or more unique protocol markers that are gen-  
15 | erated from transformation during protocol encoding and the second signature has  
16 | one or more unique protocol markers that are generated from transformation dur-  
17 | ing protocol encoding, and

18 | a signature comparison module configured to compare the first signature  
19 | with the second signature; and

20 | a cache on the local storage-system-server, the cache configured to store the first  
21 | content and to store the second content if the signature comparison module determines  
22 | the first signature of the first content and the second signature of the second content do  
23 | not match.

1 | 11. (Currently Amended) An apparatus for comparing a first content with a second con-  
2 | tent, the apparatus comprising:

3 | means for storing the first content in a cache on a local storage-system-server;

4 | means for requesting a second content from a remote storage-system-server,

5 | wherein the second content is stored in a network storage arrangement on the remote  
6 | storage-system-server;

7 | means for identifying a protocol encoding the first content and the second content;

8 | means for selecting a set of data segments from the first content and the second  
9 | content;

10 | means for computing a signature of the first content and a signature of the second  
11 | content, wherein the first signature has one or more unique protocol markers that are gen-  
12 | erated from transformation during protocol encoding and the second signature has one or

13 more unique protocol markers that are generated from transformation during protocol en-  
14 coding;

15 means for comparing the computed signature of the first content with the com-  
16 puted signature of the second content; and

17 means for storing ~~in the second content in the cache on the local storage system~~  
18 server, in response to determining the first content is not identical to the second content.

1 12. (Original) The apparatus of claim 11 wherein the selected data segments comprises  
2 locations associated with one or more protocol markers.

1 13. (Previously Presented) The apparatus of claim 11 wherein the means for computing  
2 the signature of the first content and the signature of the second content further com-  
3 prises:

4 means for identifying the one or more protocol markers associated with the first  
5 content; and

6 means for identifying the one or more protocol markers associated with the sec-  
7 ond content.

1 14. (Original) The apparatus of claim 13 wherein the one or more protocol markers as-  
2 sociated with the first content comprises discrete cosine coefficients.

1 15. (Original) The apparatus of claim 13 wherein the one or more protocol markers as-  
2 sociated with the second content comprises discrete cosine coefficients.

1 16. (Original) The apparatus of claim 13 wherein the one or more protocol markers as-  
2 sociated with the first content comprises motion vectors.

1 17. (Original) The apparatus of claim 13 wherein the one or more protocol markers as-  
2 sociated with the second content comprises motion vectors.

1 18. (Original) The apparatus of claim 13 further comprises:  
2 means for identifying a length of the first content; and  
3 means for identifying a length of the second content.

1 19. (Currently Amended) A method to compare a first content with a second content in a  
2 network storage environment, comprising:  
3 receiving the first content from a remote storage system, where the remote storage  
4 system stores the first content and other data in a network area storage arrangement;  
5 computing a signature of the first content, wherein the signature of the first content  
6 has a set of protocol markers that are generated from transformation during protocol en-  
7 coding;  
8 storing ~~in~~ the first content in a cache on a local storage system;  
9 transmitting a signature of a second content followed by the second content from a  
10 remote storage system to the local storage system, wherein the second content is stored in  
11 a network storage arrangement on the remote storage system;  
12 comparing the computed signature of the first content with the signature of the second  
13 content, wherein the signature of the second content has a set of protocol markers that are  
14 generated from transformation during protocol encoding;  
15 identifying, if the computed signature of the first content matches the signature of the  
16 second content, that the first content is identical to the second content; and  
17 terminating transmission of the second content, in response to identifying the first  
18 content is identical to the second content.

1 20. (Previously Presented) The method of claim 19 wherein the step of computing the  
2 signature of the first content further comprises:  
3 identifying the set of protocol markers associated with the content; and  
4 generating the signature from the identified set of protocol markers.

1 21. (Previously Presented) The method of claim 20 wherein the set of protocol markers  
2 further comprise a set of discrete cosine coefficients.

1 22. (Previously Presented) The method of claim 20 wherein the set of protocol markers  
2 further comprises one or more motion vectors.

1 23. (Original) The method of claim 19 wherein a size of the received content is utilized  
2 in creating the signature.

1 24. - 33. (Cancelled)

1 34. (Currently Amended) A network caching device adapted to utilize a signature asso-  
2 ciated with a protocol for caching decisions, the network caching device comprising:  
3 means for determining a protocol of new a content, wherein the new content is  
4 stored on one or more storage devices connected to a remote ~~storage-system~~ server  
5 that stores data in a network area storage arrangement;  
6 means for computing a signature of the new content, wherein the signature of the  
7 new content is a set of protocol markers that are generated from transformation  
8 during protocol encoding; and  
9 means for comparing the computed signature of the new content with signatures  
10 of other contents in a cache by comparing the set of protocol markers within the signature  
11 of the new content with protocol markers of other data contents in the cache, wherein the  
12 cache is located on a local ~~storage-system~~ server;  
13 means for determining the signature of the new content is not identical to signa-  
14 tures of other contents; and  
15 means for storing the new content to the cache, in response to determining the  
16 signature of the new content is not identical to signatures of other contents.

1 35. (Previously Presented) The network caching device of claim 34 wherein the means  
2 for computing a signature further comprises:

3 means for identifying the set of markers associated with the protocol associated  
4 with the new content; and

5 means for obtaining appropriate markers associated with the content.

1 36. (Previously Presented) A method, comprising:

2 storing a first content in a cache on a local storage system;

3 transmitting a second signature of a second content followed by the second con-  
4 tent from a remote storage system to the local storage system, wherein the second content  
5 is stored in a network storage arrangement on the remote storage system;

6 identifying a protocol encoding of the first content and the second content;

7 identifying a first signature of the first content and a second signature of the sec-  
8 ond content, wherein each signature contains one or more protocol markers identifying  
9 the content, where the one or more protocols are generated from one or more transforma-  
10 tions of each content during protocol encoding;

11 comparing one or more protocol markers within the first signature and the second  
12 signature to determine whether the first content is identical to the second content; and

13 terminating transmission of the second content from the remote storage system, in  
14 response to determining the protocol markers of the first content and the second content  
15 are identical.

1 37. (Previously Presented) The method of claim 36, further comprising:

2 computing the first signature of the first content as the first content is converted  
3 from raw data to the protocol; and

4 computing the second signature of the second content as the second content is  
5 converted from raw data to the protocol.

1 38. (Previously Presented) The method of claim 36, further comprising:

2 continuing transmission of the second content, if the first content and the second  
3 content are not identical.

1 39. (Previously Presented) The method of claim 36, wherein the one or more protocol  
2 markers associated with the first content comprises discrete cosine coefficients.

1 40. (Previously Presented) The method of claim 36, wherein the one or more protocol  
2 markers associated with the second content comprises discrete cosine coefficients.

1 41. (Previously Presented) The method of claim 36, wherein the one or more protocol  
2 markers associated with the first content comprises motion vectors.

1 42. (Previously Presented) The method of claim 36, wherein the one or more protocol  
2 markers associated with the second content comprises motion vectors.

1 43. (Previously Presented) The method of claim 36, further comprising:  
2 identifying a length of the first content; and  
3 identifying a length of the second content.

1 44. – 46. (Cancelled)

1 47. (Previously Presented) A method, comprising:  
2 storing a first file in a cache on a local storage system, wherein the first file has a  
3 first signature with a first set of protocol markers that are generated from transformation  
4 during protocol encoding;  
5 computing a signature of the second file, wherein the second signature has a sec-  
6 ond set of protocol markers that are generated from transformation during protocol en-  
7 coding;



transmitting the signature of the second file followed by the second file from a remote storage system to the local storage system, wherein the second file is stored in a network storage arrangement on the remote storage system;  
identifying a protocol type of the second file;  
comparing the first set of protocol markers to the second set of protocol markers;  
determining if the first set of protocol markers match the second set of protocol markers;  
in response to determining the first set of protocol markers match the second set of protocol markers, terminating transmission of the second file from the remote storage system to the cache on the local storage system; and  
in response to determining the first set of protocol markers do not match the second set of protocol markers, storing the second file in the cache.

48. (Previously Presented) The method of claim 47, further comprising:

in response to determining the first set of protocol markers do not match the second set of protocol markers, flushing the first file from the cache.

49. (Currently Amended) A system, comprising:

a local ~~storage system~~ server with a cache, the cache configured to store a first file, wherein the first file has a first signature with a first set of protocol markers that are generated from transformation during protocol encoding;

a remote ~~server storage system~~ server storage system configured to store a second file on one or more storage devices connected to the remote ~~server storage system~~ server storage system in a network area storage arrangement, wherein the second file has a second signature with a second set of protocol markers that are generated from transformation during protocol encoding;

a network adapter on the local ~~server storage system~~ server storage system to send a request for the second file to determine if the second file is an updated copy of the first file ~~is available~~;

a second network adapter on the remote ~~server storage system~~ server storage system to transmit a second file to the local ~~server storage system~~ server storage system; and

13 | a content comparator within the local server storage system, the content compara-  
14 | tor configured to identify a protocol type of the second file, to compare the first set of  
15 | protocol markers to the second set of protocol markers, to determine the first set of proto-  
16 | col markers match the second set of protocol markers, in response to determining the first  
17 | set of protocol markers match the second set of protocol markers, to terminate transmis-  
18 | sion of the second file to the cache, and in response to determining the first set of proto-  
19 | col markers do not match the second set of protocol markers, to store the second file in  
20 | the cache and flush the first file from the cache.